SECURED APPLICATION BASED MOBILE BANKING SYSTEM FOR NIGERIA

BY

FAISAL ALI GARBA
P14SCMT8048
+234 080 36028632, alifa2try@gmail.com

A DISSERTATION PROPOSAL PRESENTED TO THE DEPARTMENT OF MATHEMATICAL SCIENCE,
FACULTY OF SCIENCE, AHMADU BELLO UNIVERSITY, ZARIA. AS PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE

FEBRUARY, 2016

Abstract

This dissertation proposes a secured application based mobile banking based on a three level authentication mechanism: i. what the user knows (Bank Verification Number (BVN), ii. what the user has (his/her mobile phone's Media Access Control (MAC) address iii. what the user is (user's fingerprints and finger vein multimodal biometric data). This proposal ensures secured transmission of data using Kerberized LDAP and Advanced Encryption Standard for authentication and encryption.

Chapter One

Introduction

1.1 Background of the Study

Three billion Internet (3) users were likely to be realized by May 2015. Mobile Internet penetration is forecast to reach 71% by 2019. One hundred and ninety two (192) countries have active 3G mobile networks, which cover almost 50% of the global population. Smartphone sales are the majority of mobile handsets sold worldwide; tablet sales will soon exceed total PC sales. While there are at least five mobile platforms, Android has an 84% share of smartphones, and 72% of tablets. There are well over 1 million apps available, which have been downloaded more than 100 billion times. Time spent using apps exceeds time spent on mobile browsers, and in the US, at least, exceeds time spent on desktop and mobile browsers combined (Internet Society, 2015).

Mobile banking is defined as the service which qualifies customers to receive information about their accounts and to make real transactions by using mobile phones in a secure and reliable way. Services like: enquiry (balance enquiry/ mini statement/ currencies rates), money transfer, bill payment, cheque book request and many other banking services (El-Safi, 2013). Growth in the M-Banking is driven by various facilities like convenience of banking operations, greater reach to consumers and integration of other m-commerce services with mobile banking. In M-banking there is no place restriction, it is highly penetration coefficient as growth of mobile phones are more than computers, it is fully personalized and private increasing transaction authenticity and is 100% available all the time with users (Pujitha &

Mallu, 2013). M-banking can be executed using various channels like SMS, USSD, GPRS, WAP; Phone based Application, SIM Application. All of these channels are used separately or combined for various banking operations:

A. Short Message Service (SMS)

SMS is the simplest form of mobile banking. It is largely used for information-based services.

B. Unstructured Supplementary Services Delivery (USSD)

USSD is a technology unique to GSM. It is a capability built into the GSM standard for support of transmitting information over the signaling channels of the GSM network. USSD provides session-based communication.

C. Wireless Application Protocol (WAP) /General Packet Radio Service (GPRS)

GPRS is a packet-switched data service available to GSM users. GPRS enables services such as WAP access, Multimedia Messaging Service (MMS), and Internet communication services such as email and World Wide Web access in mobile phones. WAP is wireless application protocol used over GPRS. It is similar to Internet banking. The consumer's handset needs to be WAP enabled. WAP banking is open to similar threats as Internet banking.

D. Phone-based Application

Phone based applications are developed in various languages like J2ME and .NET having advantages that it can use GPRS, USSD or SMS,

MMS to carry the consumer data/instruction in an encrypted format and it is operator independent. These are secure application which resides on supported handset.

E. SIM Application Tool Kit

The SIM Application Toolkit allows for the service provider or bank to house the consumer's mobile banking menu within the SIM card. STK is the most secure method of mobile banking. It allows the bank to load its own encryption keys onto the SIM card with the bank's own developed application (Pujitha & Mallu, 2013).

A questionnaire was created by (Kaya, 2013)as an attempt to understand the difference in behavior and to gather a sense of trust in mobile banking. The sample data revealed that more than 70% use mobile applications in general. The vast majority (77%) of users were concerned with security regarding mobile banking services and that is the main reason for not using mobile banking in 40% of the cases while the other 37% are still concerned but use it anyway (Kaya, 2013). The results of the questionnaire also revealed that only 30% of users carry out banking transactions via mobile browser or mobile banking application. 70% of the ones that carry out mobile banking prefer to use a mobile bank app. A possible reason for that could be because of its ease to use or maybe because of their trust in the mobile bank app which is a direct link to the bank instead of using a browser (third-party) in between the customer and the bank. 40% were unsure about the mobile banking application security level, but when asked about the online banking (using a browser) 92% believed that the level of security provided was medium or high. The sample data shows the sense of trust

in online banking is much higher than the one of the banking application (Kaya, 2013). Applications can be considered safer than accessing banking account through a web browser. Apps provide a direct link from the device to the bank, without having to go through any additional browser or third-party applications. This means banks have better control over the security and connection with customer interactions. Because these apps are built specifically for a particular bank and its customers, the bank can provide a secure connection using SSL encryption, two-factor authentication and other elements to redeem the application secure for use (Kaya, 2013).

Mobile bank apps provide a direct link from the device to the bank, without having to go through any additional browser or third-party application. This means banks have much better control over the security and connection of customer interactions. Because these apps are built specifically for a particular bank and its customers, the bank can provide a secure connection using SSL encryption and two-factor authentication that meets the institution's unique needs. Even if someone is able to obtain a customer's phone, they will still be required to put in a username and password, and if available, provide a second factor of authentication, in order to gain access to the accounts. Along with these two factors of authentication, many banks have started implementing a third method of security: a profile of a customer's actions. Banks and other financial institutions are able to monitor a customer's actions when banking via a mobile app, creating a profile of those interactions. Another plus to using a mobile application is the fact that most smartphones and tablets can now be cleared or reset from remote locations. Thus, if someone steals or obtains a mobile device,

the customer can use his or her computer or any other device with an Internet connection to clear any data and apps from the device, eliminating the possibility that someone else can use the phone to access the customer's account. As customers become more familiar with mobile banking app security and learn to trust a bank's mobile app brand, they will be more willing to use these tools (Kaya, 2013).

Due to advancement in technology, customers and organizations take interest in biometrics technology to reduce the uncertainty and security concern. Biometrics authentication mechanism is to identify the physical individuality or uniqueness of the authorized person (R. & M.A., 2009). The advantage of using finger print is that, communication can occur only through authorized persons and will be secure. Finger print technology is the most commonly used in telecommunication industry (Krevatin, 2010). If finger-print technology is introduced in mobile phones, then the risk of unauthorized persons using the mobile for mobile banking is significantly reduced (Bilal & Sankar, 2011). Finger-print takes only 256 bytes and its accuracy is high. The biometric device first captures the user's finger print and creates a reference template and it is stored in database and that ends the enrolling processes of user's finger print (Michaels, 2008).

The concept of multimodal biometric system has gained enormous attention because of their reliable and accurate identity verification. Multimodal biometric systems based on fingerprint and finger vein modality provide promising features useful for robust and reliable identity verification. Among the different biometric modalities that can be used to constitute a multimodal biometric system the use of fingerprint

and finger vein appears to be more refined because: (1) The human fingers are highly convenient for imaging and disclose variety of features when captured in different spectrums. For instance, imaging the finger with visible spectrum will disclose the texture features present on the finger surface that in turn can be used to extract minutiae features of the fingerprint or the line features of the whole finger. While imaging the finger with a near infrared spectrum will allow one to capture the finger vein pattern. (2) Low verification error rates can be achieved by combining these complementary features available from the single biometric modality i.e, finger. (3) Use of finger-vein shows strong anti-spoofing nature as it is hidden inside the finger and cannot be stolen without subject co-operation. (4) The two biometric characteristics can be acquired with one capture device and in principle with a single capture attempt (Raghavendra, Raja, Surbiryala, & Busch).

Bank Verification Number (BVN) is an initiative of the Central Bank of Nigeria. It is a scheme initiated to address the increasing incidents of compromise on conventional security systems (password and PIN). The Central Bank of Nigeria through the Banker' Committee and in collaboration with all banks in Nigeria on February 14, 2014 launched a centralized biometric identification system for the banking industry tagged Bank Verification Number (BVN) (Home, 2016). Amongst the benefits of BVN are:

1. BVN gives a unique identity that can be verified across the Nigerian Banking Industry (not peculiar to one Bank)
2. Customers bank accounts are protected from unauthorized access
3. It will address issues of identity theft, thus reduce exposure to fraud

The purpose of the project (BVN) is to use biometric information as a means of first identifying and verifying all individuals that have account(s) in any Nigerian bank and consequently, as a means of authenticating customer's identity at the point of transactions. To provide a uniform industrially accepted unique identity for Bank Customers and to authenticate transactions without the use of cards using only biometric features and PIN (Home, 2016).

A unique ID number is to every bank customer at enrolment and linked to every account that the customer has in ALL Nigerian Banks. Individuals are required to submit an acceptable means of identification as prescribed for enrolment. During enrollment all ten (10) fingers and facial image are captured. For authentication purposes, individuals performing banking transactions are required to identify themselves using their biometric features which will be matched against information in the central database. To enroll for BVN customers are required to walk into any branch of their bank to fill out and submit the BVN Enrolment form. They are then required to present themselves for biometric data capturing (such as fingerprint, facial image etc). An acknowledgment slip with the transaction ID is issued to customer and within 24 hours the system confirms customer's application, the BVN is generated and an SMS is sent to him for pickup. The BVN and unique features of an individual shall be used in conjunction with a PIN on a point of transaction (Home, 2016).

Security has become a primary concern in order to provide protected mobile transaction between the clients and the bank servers. Secure authentication of client information depends on some fundamental

security approaches which will not jeopardize the client sensitive information. This has led to different researches ranging from single-factor authentication, two-way authentication, and multifactor authentication. Bearing in mind the cost of providing these services to clients, most banks are wary of balancing profit making and security. In Nigeria today, most mobile banking applications use the single-factor authentication which consist of the username and password. The single-factor authentication is prone to attacks, in cases of theft or perceived trusted third parties, the security can be breached with ease. Password hackers can easily break the security since most passwords are weak. Some customers using the online banking system in Nigeria have experienced unauthorized access to their banking information and, in some cases, unauthorized withdrawal from their accounts. Secure mobile banking will build confidence in customers knowing that their information is secure and they can carry out secure transactions without fear of man-in-the-middle attacks. Though the issue of theft strongly depends on how a client protects his/her mobile phone device from third parties. The future of Nigerian banking is mobile, due to the availability of mobile phones to remote customers in the villages, towns and places where banks or ATMs are not in close reach for customers. The proposed cashless society in Nigeria will propel this future as fast as possible for Nigeria to be recognized among world players in financial and technological innovations (Adesuyi, Oluwafemi, Oludare, Victor, & Rick, 2013).

1.2 Definition Of The Problem

Nigeria has over 150 million mobile subscribers (NCC, 2016). It can be expected that a percentage of this population, considering the government penchant for a cashless society, would embrace the mobile banking option.

From a survey carried out by (Research, 2010), 20% of respondents revealed they employ mobile banking platform. Though, the level of mobile banking adoption in the country is still relatively young, many of the banks currently provide mobile banking platforms for customers (Research, 2010). From observations, the platforms provided by these banks require only username and password to gain access. Considering the fact that no system is perfect, mobile banking, like every other type of banking like ATM, credit card, mobile money, despite its immense benefits, is also not immune to security challenges. Yet, there is need for the available platforms to effectively control application and data access (Association, 2009), hence the need for multi-factor level of authentication. This is necessary to encourage customers to embrace mobile banking. (Komolafe, Agwuegbo, & Agunlehin, 2009).

According to Nigeria Deposit Insurance Commission (NDIC) report on electronic and related frauds for the quarter end of 2008 the incidence of frauds in banks maintained an upward surge. A typical example is the bank-wide increase in cases of ATM fraud. This is in spite of efforts by Interswitch and member banks to raise awareness (Komolafe, Agwuegbo, & Agunlehin, 2009). In 2008, the Economic and Financial Crimes Commission reports ranked Nigeria as the third among top ten source of electronic related fraud in the world. A society like Nigeria would be engulfed by electronic fraud if the system is not checked. These cases and statistics mentioned above have prompt the need to develop a secured mobile banking platform. This is also in line with the Central Bank's drive for a cashless society (Adesuyi, Oluwafemi, Oludare, Victor, & Rick, 2013).

1.3 Aim

The aim of this research is to create a secured application based mobile banking system for Nigeria based on a three-level authentication mechanism.

1.4 Objectives

1. To ensure a secure transmission of bank customer's data to protect it from man in the middle attacks.

2. To provide an application based mobile banking model that utilizes the Bank Verification Number policy of the Central Bank of Nigeria.

3. To develop a user friendly interface to encourage customers to carry out their banking transactions in an easy way.

4. To ease and simplify banking transactions and make them more attractive to customers through a user friendly android application.

5. To reduce the number of queues in banks.

1.4 Method Of Achieving The Objectives

1. Android mobile application shall be developed as a client. This application will make use of stubs (proxies) to connect to a web service application to retrieve data.

2. A web service shall be developed using Java to work like a mediator between mobile client application and the bank server.

3. Stubs are generated by passing the web service WSDL (Web Service Description Language) to a Stub generator program (KSoap2).

When the Android application is run, a number of sequential operations take place as follows:

1. Mobile client application prompts the user to enter his 11 digits BVN to login to the mobile banking app.
2. Next the mobile client application will require the user to scan any of his fingers for authentication.
3. A preliminary authentication (client level) using the BVN only, is conducted at the application level and if it returns positive, the mobile application sends the device MAC (Media Access Control) address, fingerprint and BVN to the authenticating Kerberos Server for ticket granting.
4. When the Kerberos Server confirms the identity and permissions of the device and the user, the ticket granting process begins.
5. If the ticket granting is successful, the application automatically connects to the mobile banking server using the ticket granted by the Kerberos Server.
6. Mobile application client call the web service through the stubs
7. Mobile client application prompts the user to navigate through different services.
8. For every transaction, the customers' initial access BVN serves as a transaction confirmation number, which they must input to confirm

each transaction.

9. The banking server and the mobile device use a symmetric key (Advanced Encryption Standard) known only to the two communicating devices to encrypt and decrypt transaction information.
10. Once the customer selects logout on the menu, the ticket expires, the communication between the server and the mobile device expires and the mobile application is closed automatically, after notifying the user, signaling the end of operation.

The server also should initiate a session to keep track of the authenticated customer and a cookie also should be saved in mobile application. An automatic logout is carried out if the client becomes idle for a long time (El-Safi, 2013).

Functions to be developed in the web service:

1. Log in and authentication function (El-Safi, 2013)

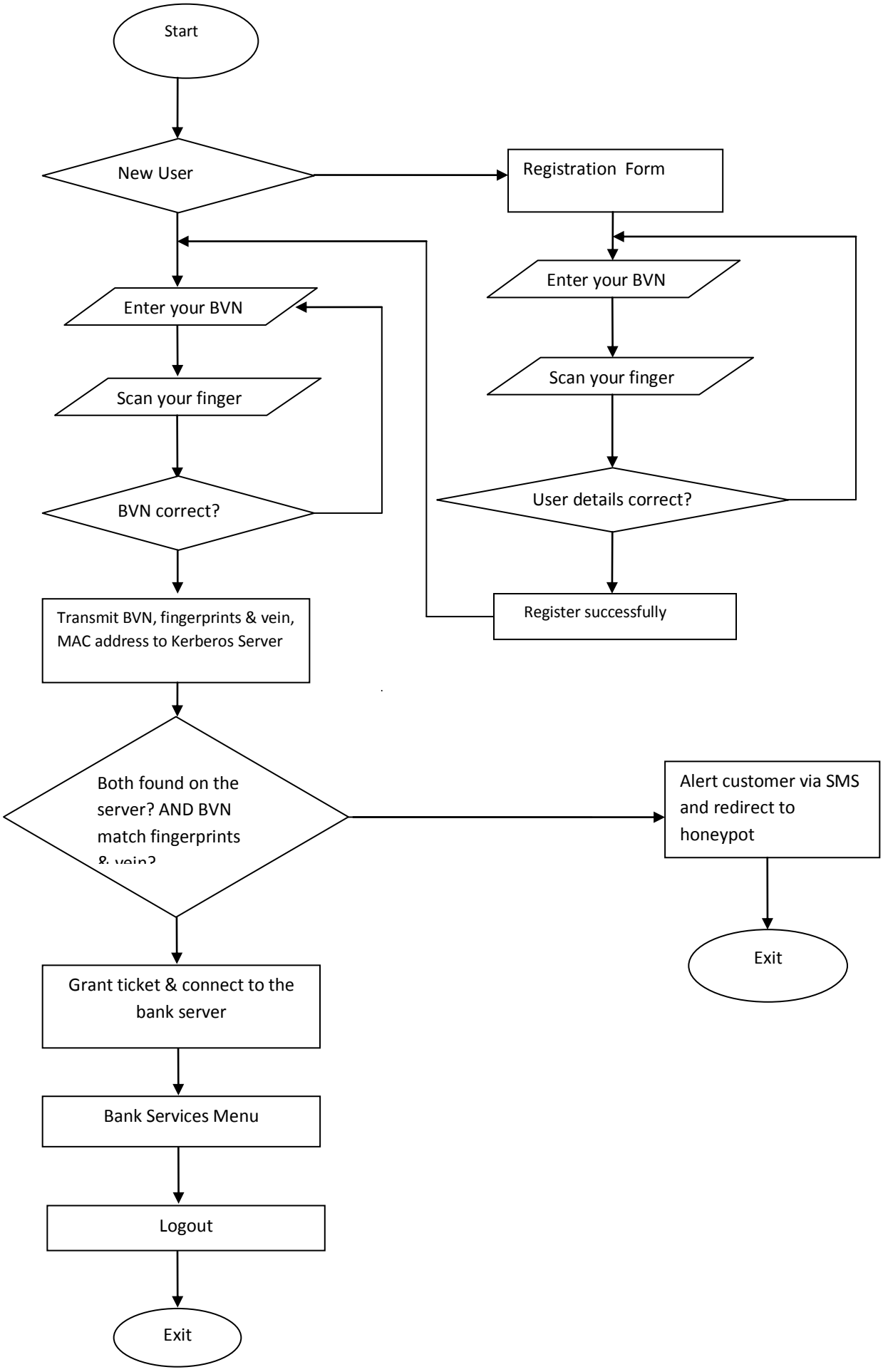
2. Sign up function

3. Balance inquiry function

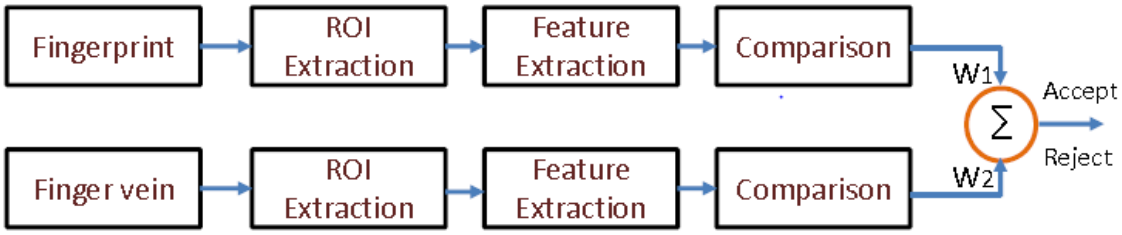
4. Send money

5. Help function

6. Transaction history function


Start
New User
Registration Form
Enter your BVN
Scan your finger
User details correct?
Register successfully
Enter your BVN
Scan your finger
BVN correct?
Transmit BVN, fingerprints & vein, MAC address to Kerberos Server
Both found on the server? AND BVN match fingerprints & vein?
Alert customer via SMS and redirect to honeypot
Exit
Grant ticket & connect to the bank server
Bank Services Menu
Logout
Exit

It is the dissertation expectation that mobile phone manufacturers would come up a with mobile phones that have sensors capable of capturing both fingerprint and finger vein simultaneously. Such sensor proposal has been presented by (Raghavendra, Raja, Surbiryala, & Busch).



Block Diagram of the Proposed Verification Scheme. (Raghavendra, Raja, Surbiryala, & Busch)

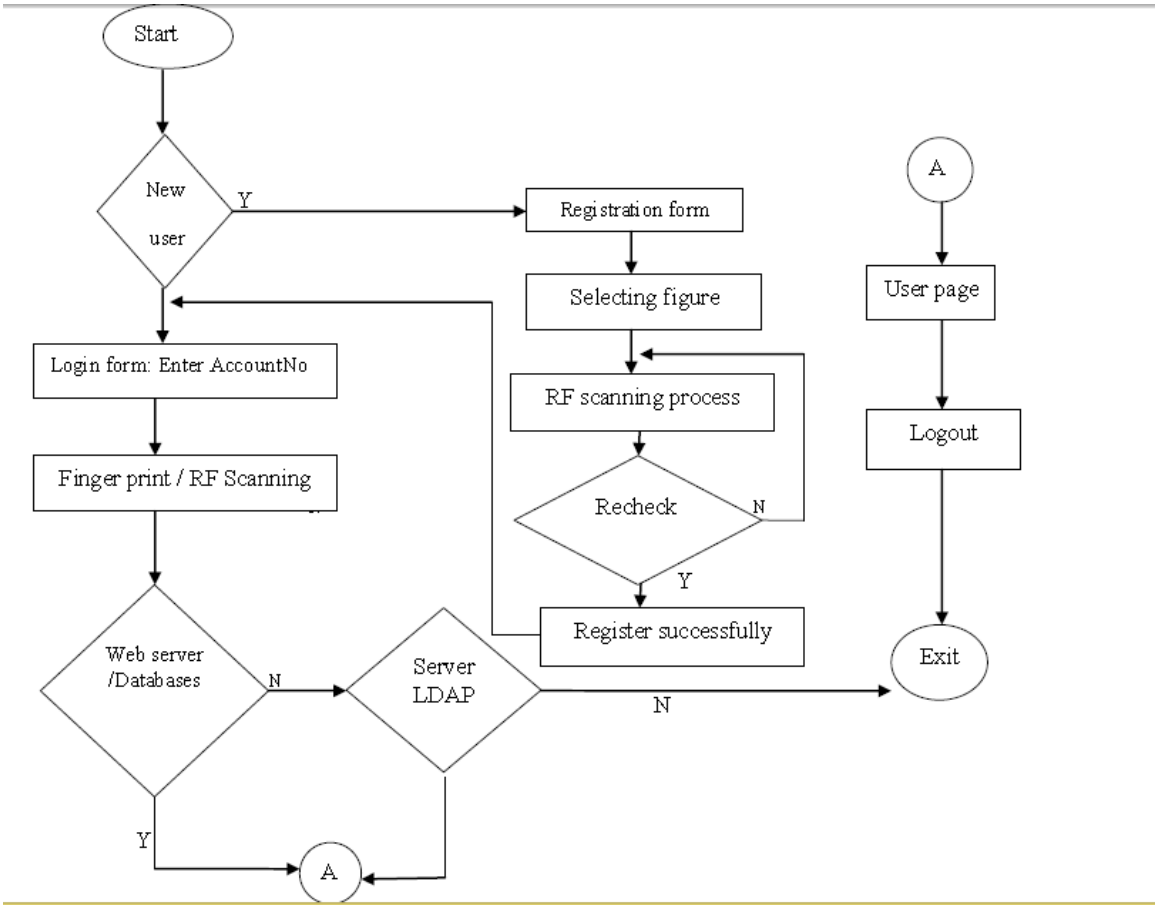
My dissertation also assumes that similar fingerprint and finger vein might have been captured in the course of enrolment, during the BVN registration. I will however, use some numbers to represent the biometric data both at the enrolment and verification stage, since the hardware to support the multimodal biometric data capture is not available at the moment.

Chapter Two

Literature Review

2.1 Introduction

A biometric based mobile banking was proposed by (Bilal & Sankar, 2011). Their proposal work thus: There are two types of users (1) registered users (2) new users. The registered users will directly go to login form while the new users will go to registration form. They proposed scanner that utilizes Radio Frequency (RF) scanning. Their reason is that with RF scanning, it is possible to differentiate between living cells and dead or copied cells. After the verification of data, the customer will be able to access the database through web server. If the finger print matches with that of the database then customer will be able to start mobile banking services through mobile handset. For additional security Lightweight Directory Access Protocol (LDAP) server is used. If first finger prints authentication is not found in database then it will be checked in LDAP server for more verification.



Flowchart of the proposed mobile banking system (Bilal & Sankar, 2011)

A flowchart of their proposal is presented above. New users are required to register any three finger print in database and also need to fill in a registration form. If the finger print of the bank customer is registered successfully then customer will be able to use mobile bank services.

For secure authentication purposes they proposed finger print scanner device. Mobile manufacturing companies will make the biometric scanner device with mobile hand set. The mobile customer will used it for authentication purposes. After capturing finger print, the data will be transmitted through internet. And the data can be accessed through bank

server. The finger print scanner device can be attached to mobile phone though a port. They narrated that the process which statistically gives the best possible template is called *consolidation*. Consolidation of three finger template produce high quality enrolled template according to Statistical Research, they reported. With the help of the finger scanner device, mobile handset gets three samples as shown in the figure. These samples are stored in bank server with appropriate account holder. In case of cut, burn, damage of one finger the other finger print data will still serve as a unique identifier they claimed. Finger print is present for matching in the database record. Every time new finger print is compared to the stored finger print.

For authentication purposes and to secure customer data at server end additional server known as Server LDAP authentication is used. In LDAP, the client sends the query packet through TCP/IP to the server. The server confirms the identifier on LDAP Directory Information Tree (DIT) which is stored on LDAP server. When the result is found, it is sent back to client. In case of result not found then query will be sent to another LDAP server. This LDAP verify the data in tree model structure method. They claimed that LDAP authentication has many advantages like centralized usage, privileges, management, and storage of user information and user accounts (Bilal & Sankar, 2011).

My proposal differs with theirs in the following ways: first, my mobile banking proposal utilizes an application not a WAP browser. And according to (Kaya, 2013), mobile banking through applications is regarded safer than accessing banking account through a web browser. Furthermore, applications provide a direct link from the device to the bank, without

having to go through any additional browser or third-party applications. This means banks have better control over the security and connection with customer interactions. Because these apps are built specifically for a particular bank and its customers, the bank can provide a secure connection using SSL encryption, two-factor authentication and other elements to redeem the application secure for use (Kaya, 2013). Secondly, my proposal uses Kerberos and not LDAP server. The use of LDAP software in its current state is not suitable as an authentication service as shown by (Obimbo & Benjamin, 2011). The two fundamental flaws of LDAP as shown by (Obimbo & Benjamin, 2011) include LDAP servers DoS attacks and user passwords discovery over a network. The use of Kerberos as better alternative authentication service over LDAP has been suggested by (Obimbo & Benjamin, 2011).

A mobile client application that uses wireless access protocol to enable customers securely transmits banking information was proposed by (El-Safi, 2013). He proposes a MIDlet (Java 2 Micro Edition) application that will transmits banking information through a secure communication path. The MIDlet role was to prevent unauthorized access by imposing login form that connects to backend database to investigate from it the identity of the entered user, then allows the user to proceed to transactions and inquires form. He proposes an interface between the backend database and MIDlet represented in a web service, the idea of putting the web service in the middle to exploit the properties of the web services like language independence and interoperability, thus enables using any language to develop the client applications, thus the mobile application client can invoke different functions described in the web service. Web service bear effort of

dealing with the backend database and return the result to mobile application client.

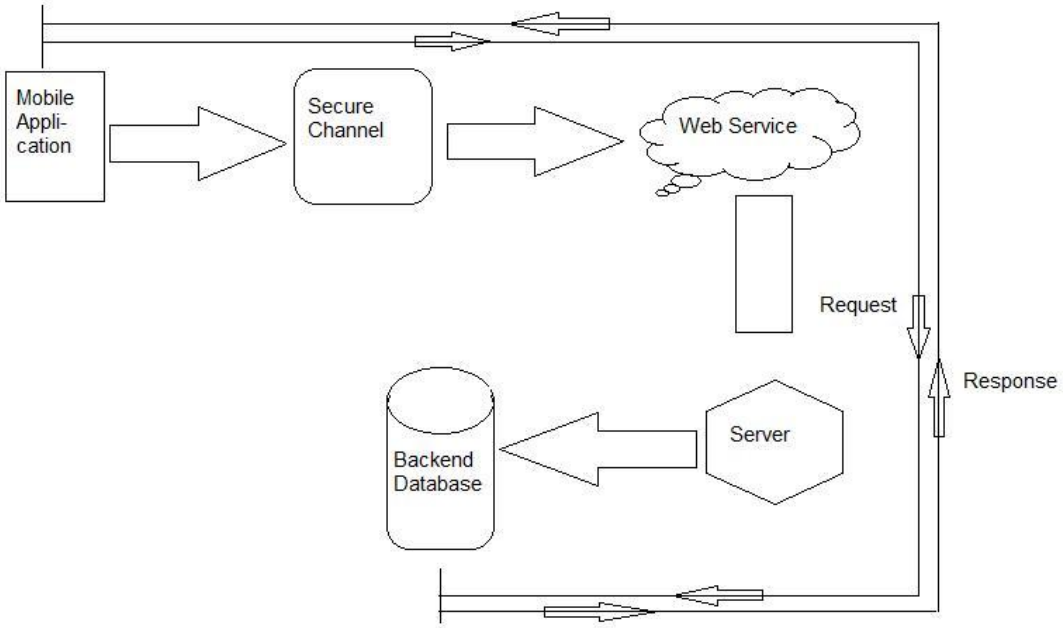
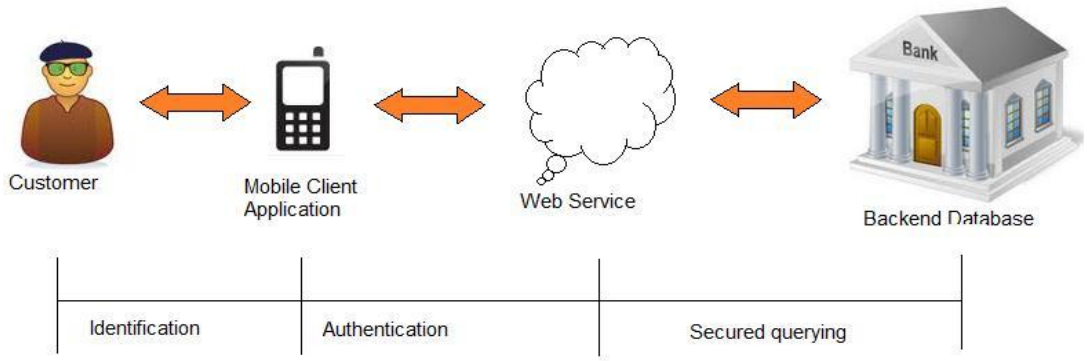


Illustration of architecture of mobile banking using application clients (El-Safi, 2013)

To ensure the security of transaction, there are three main aspects should be maintained as show in figure 5 below and reported by (El-Safi, 2013):



Modular Transaction Architecture (Hayashi & Weiner, 2003) **cited by** (El-Safi, 2013)

For identification purpose (El-Safi, 2013) proposes the use of account number which is already known by bank and customer, user name which is a unique name given to a customer, mobile pin (m-pin) a one-time password given to a customer and imposed to change it at first login, mobile application client version to help identify which version is used by the customer and to let him know if there are some upgrades, IMEI used as a log of used phones, this may help if a fraud case occurred.

To ensure the identification format integrity a message digest is generated and appended to the identification format. Digest is a digital fingerprint of block of data, as example Secure hash algorithm #1 (SHA1) there is no hope that two messages have the same SHA1 fingerprint (negligible value of duplication) .When the request reach the server side a digest is generated and compared with the appended digest, these ensure the integrity of the request. The server also should initiate a session to keep track of the authenticated customer and a cookie also should be saved in mobile application. An automatic logout is carried out if the client becomes idle for a long time (El-Safi, 2013).

A security mechanism to ensure a secure channel is implemented to protect customers' confidential data from sniffing and man in the middle attacks. The request and response between MIDlet and web service is transmitted as a plain text, thus an encryption technique must be used. He proposes the use of authentication certificates to guarantee a secure connection between client and server by using SSL connection. SSL

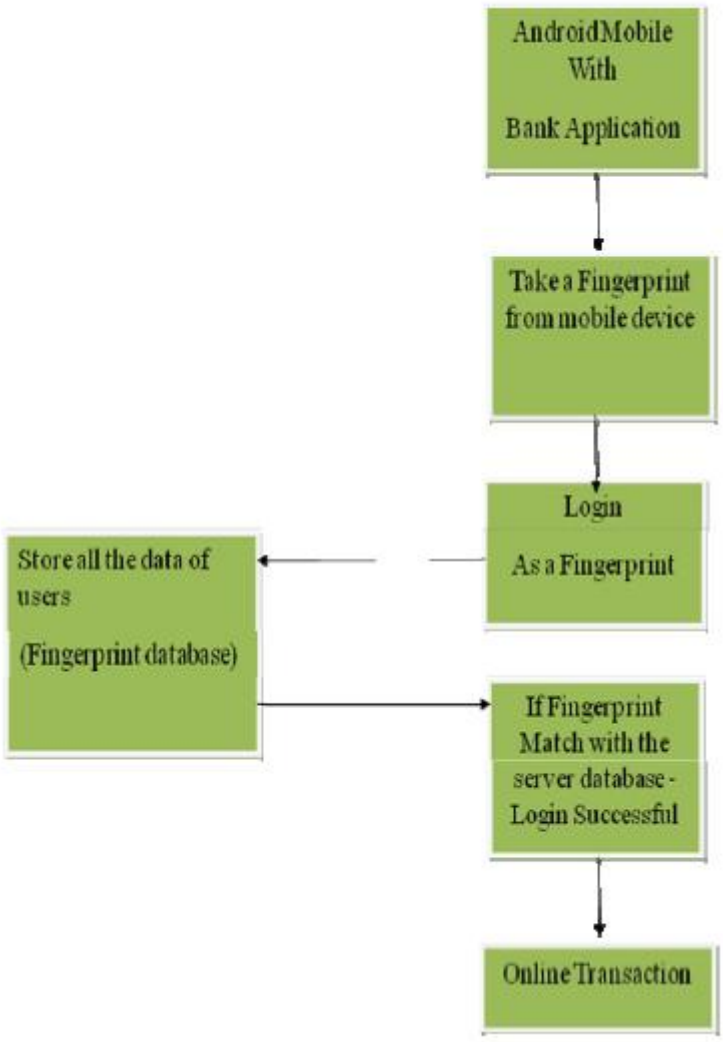
makes use of what is known as asymmetric cryptography, commonly referred to as public key infrastructure (PKI). With public key infrastructure, two keys are created, one public, one private. Anything encrypted with either key can only be decrypted with its corresponding key. Thus if a message or data stream were encrypted with the server's private key, it can be decrypted only using its corresponding public key, ensuring that the data only could have come from the server.

The bank server is responsible for respond to coming requests and it is represented by the web service which is implemented using SOAP protocol and data are represented as XML format. Web Service provides the ability to call different methods without need to about their implementation. The method signature is described by WSDL. Web service description language (WSDL) is used for describing the functionality offered by a web service; WSDL is used by MIDlet to generate Stubs that work as proxies to invoke the remote functions. The backend data base represents the container for customers' confidential information. Stored procedures are developed to be called by web service, interaction between web service and database is done through it. This enables bank to veil their database architecture. The connection between the web service and the database should be the responsibility of the bank to provide secure environment (El-Safi, 2013).

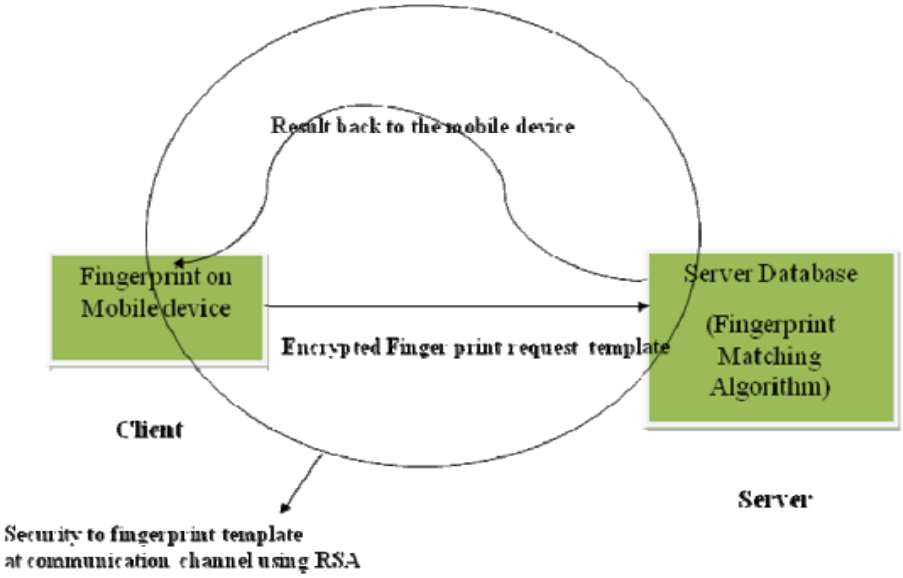
My proposal differs from that of (El-Safi, 2013) in the following ways: first, the proposal by (El-Safi, 2013) relies on only username and PIN as the client's level means of identification which are a weak means of identification when compared with biometric means of identification. My proposal uses client's 11 digit BVN and fingerprints and finger vein

multimodal biometric data. Secondly, his proposal utilizes a PKI based SSL connection to secure the transmission of data. Digital Certificates used by PKI are regarded weak as Certificates could be exported and utilized remotely. They can also be used by more than one user at a time, thus allowing the use of stolen certificates. My proposal on the other hand, utilizes AES for secured transmission of data between client and server and Kerberized LDAP for a proper authentication. Finally, his proposal uses a Java MIDlet application whereas my proposal uses an android application the most used smartphone operating system.

A biometric based mobile banking on android device was proposed by (Belkhede, Gulhane, & Bajaj, 2012). They proposed a system that captures the fingerprint of a client with the use of his/her smartphone camera. “The solution involves the use a biometric authentication mechanism. A payment application would be installed onto an android device, for authentication finger print is taken at run time. The finger print template would be captured by the phone and compared against a stored template on a database server. The fingerprint template is encrypted by using the RSA algorithms and sends it to the host server (i.e Bank). Fingerprint is used for the login purpose for the bank application on mobile”. (Belkhede, Gulhane, & Bajaj, 2012)



Flowchart of Secured Mobile Payment (Belkhede, Gulhane, & Bajaj, 2012)



Enhanced security at the client server wireless communication (Belkhede, Gulhane, & Bajaj, 2012)

“Mobile will act as a client and the bank website will act as a server (host server). Once fingerprint is taken as a login, it sent to the server for matching as request, and server send the reply message. If it is matching then only login will be successful and user can do the transaction. In the client server module for providing the enhanced security authors use the encryption technique so at the wireless transmission no one can hack the fingerprint template.” (Belkhede, Gulhane, & Bajaj, 2012)

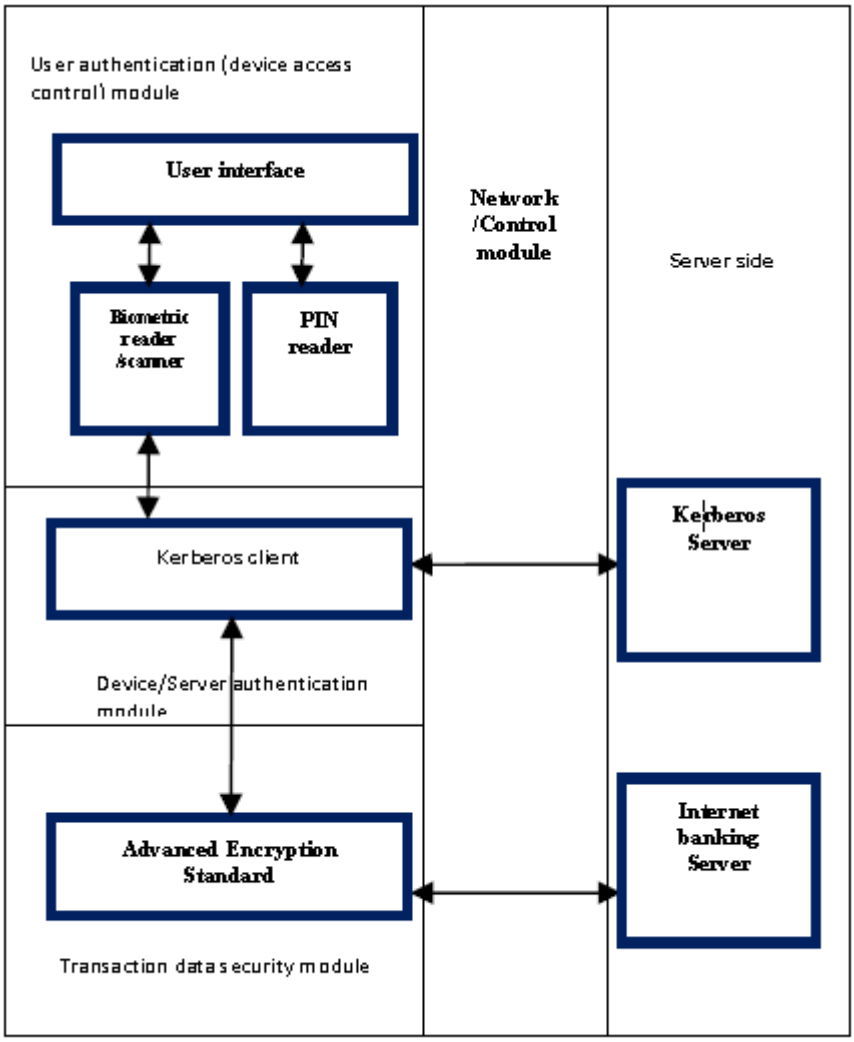
My proposal and that of (Belkhede, Gulhane, & Bajaj, 2012) differs in that my proposal entails the use of a fingerprint and finger vein multimodal biometric data. Moreover, in my proposal fingerprint data is not extracted via digital camera but via a scanner incorporated in application.

Finally the proposal of (Nwogu, 2014)that uses 3-level security for Internet banking systems using an internet banking dongle, Kerberos, Advanced Encryption Standard (AES) and Biometric Identification. His proposal has the following algorithm:

1. An intending user inserts the USB Internet banking dongle on a PC or tablet with Internet connectivity; the dongle user login interface is launched automatically.
2. The interface prompts the user to supply their PIN and fingerprint.
3. The preliminary security check (client level security) is conducted by the dongle application. And if this returns positive, the dongle application sends the information to the authenticating Kerberos server for ticket granting.
4. When the Kerberos server confirms the identity and permissions of the dongle device and the user, the ticket granting process begins.
5. If the ticket granting is successful, the dongle application automatically connects to the internet banking server using the ticket granted by the Kerberos server.
6. On the internet banking server interface, the user supplies their account login credential (username and password) to gain access to the internet banking menu where they can select operations to be performed.
7. For every transaction, the customers' initial access PIN serves as a transaction confirmation number, which they must input to confirm each transaction.
8. The internet banking server and the dongle use a symmetric key (Advanced Encryption Standard) known only to the two communicating devices to encrypt and decrypt transaction information.
9. Once the customer selects logout on the menu, the ticket expires, the communication between the server and the dongle terminates and the

dongle application is closed automatically, after notifying the user, signaling the end of the operation.

10. Customer ejects their dongle from the computer.



Modules interaction for the proposed system (Nwogu, 2014)

My proposal and his differs in that we have a different means of implementation. His proposal works on a dongle whereas mine uses a mobile device application. In addition, his target was the security of Internet

Banking whereas mine is mobile application based banking. Secondly, his proposal utilizes fingerprints identification alone, whereas mine proposes a fingerprint and finger vein multimodal biometric identification the client's fingers.

CONCLUSION

This outcome of this dissertation is a complete model for a three level secured application based mobile banking model for Nigeria, which will cater for all the security requirements i.e. confidentiality, integrity, authentication & authorization, non-repudiation, access control.

Although mobile client application increase development life cycle regarding to different combinations of devices and operating systems and different mobile phones capabilities and performance and also increase in customer service and support issues; but it offers organization more control over the user experience, with a rich user interface capability. Also it gives the ability to work even when there is no connection to wireless network for the customers (some offline services, e.g. ATM location). Moreover secure connection can be established between the server and the application (El-Safi, 2013).

FUTURE RESEARCH

1. Investigate the security of a mobile banking application through pervasive parallelism.

RESEARCH PLAN

ID	Task Name	Finish
1	First Proposal Defence	March 01
2	Second Proposal Defence	March 14
4	Bank Server Design & Development	April 28
5	Mobile Applications Design & Development	June 14
12	Web Services Development	June 30
13	Implementation Running	July 1
14	Final Report Draft	July 30
15	Internal Defence Seminar	August 1
16	External Defence Seminar	August 14

Deliverables

1. Complete Project Reports
2. CDs with Complete Project Source Codes

Bibliography

Adesuyi, F. A., Oluwafemi, O., Oludare, A. I., Victor, A. N., & Rick, A. V. (2013). Secure Authentication for Mobile Banking Using Facial Recognition. *IOSR-JCE*, 51-59.

Association, M. B. (2009). *Mobile Banking Overview.*

Belkhede, M., Gulhane, V., & Bajaj, D. P. (2012). Biometric Mechanism for Enhanced Security of Online Transaction on Android System: A Design Approach. *ICACT2012.*

Bilal, M., & Sankar, G. (2011). *Trust & Security Issues in Mobile Banking and it's Effect on Customers.* Karlskroma: Blekinge Institute of Technology.

El-Safi, A. A. (2013). *Mobile Banking Project.* Sudan: Faculty of Mathematical Sciences, University of Kharthoum .

Hayashi, F., & Weiner, S. E. (2003). *A Guide to the ATM and Debit Card Industry.* Federal Reserve Bank of Kansas.

Home. (2016, 01 01). Retrieved 01 01, 2016, from http://www.bvn.com.ng/

Internet Society. (2015). *Mobile Evoulution and the Development of the Internet.* Internet Society.

Kaya, M. M. (2013). *Trust and Security Risks in Mobile Banking.* Kellogg College, University of Oxford .

Komolafe, B., Agwuegbo, A., & Agunlehin, T. (2009). *Nigeria: Banks' Customers Agonise as ATM Fraud Persist*. Retrieved from www.allafrica.com/stories/200911300313.html

Krevatin, I. (2010). Biometric Recognition in Telecom Environment. *Intelligence in Next Generation Networks (ICIN).* Berlin: IEEE.

Michaels, L. (2008). Biometric Security for Mobile Banking.

NCC. (2016, 01 01). *Index*. Retrieved 01 01, 2016, from www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:subscriber-statistics&catid=65:industry-information&item=73

Nwogu, E. R. (2014). Improving the Security of the Internet Banking System Using Three-Level Security Implementation . *IJCSITS*.

Obimbo, C., & Benjamin, F. (2011). Vulnerabilities of LDAP as an Authentication Mechanism . *Journal of Information Security*, 151-157.

Pujitha, S., & Mallu, B. V. (2013). SMS Based Mobile Banking. *IJETT*.

R., T., & M.A., K. (2009). Improving E-Banking Security with Biometrics:Modelling User Attitudes and Acceptance. *New Technologies, Mobility & Security (NTMS), 2009 3rd International Conference.* Cairo: IEEE.

Raghavendra, R., Raja, B. K., Surbiryala, J., & Busch, C. (n.d.). A Low Cost Multimodal Biometric Sensor to Capture Finger Vein and Fingerprint.

Research, P. (2010). The Impact of Mobile Services in Nigeria.

Slezak, D. J., & Seeborg, M. (2002). The Cellular Divide: A Comparative Analysis of Mobile Phone Usage in Spain and the United States . *John Wesley Powell Student Research Conference*. Illinois.